Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography

Neha Tirthani
School of computing Sciences and Engineering,
M. tech. – Computer Science,
VIT, Chennai campus,
neha.tirthani2013@vit.ac.in

Ganesan R
School of computing Science and Engineering,
Associate Professor (CSE),
VIT, Chennai campus,
ganesan.r@vit.ac.in

***Abstract* – Technological advancements in cloud computing due to increased connectivity and exponentially proliferating data has resulted in migration towards cloud architecture. Cloud computing is technology where the users' can use high end services in form of software that reside on different servers and access data from all over the world. Cloud storage enables users to access and store their data anywhere. It also ensures optimal usage of the available resources. With a promising technology like this, it certainly abdicates users' privacy, putting new security threats towards the certitude of data in cloud. The security threats such as maintenance of data integrity, data hiding and data safety dominate our concerns when the issue of cloud security come up. The voluminous data and time consuming encryption calculations related to applying any encryption method have been proved as a hindrance in this field. In this research paper, we have contemplated a design for cloud architecture which ensures secured movement of data at client and server end. We have used the non breakability of Elliptic curve cryptography for data encryption and Diffie Hellman Key Exchange mechanism for connection establishment. The proposed encryption mechanism uses the combination of linear and elliptical cryptography methods. It has three security checkpoints: authentication, key generation and encryption of data.**

Index Terms – cloud architecture, ECC, Diffie Hellman

I. Introduction

Defining cloud computing becomes a difficult task with many definitions, yet no consensus on single or unique ones. Cloud computing refers to a network of computers, connected through internet, sharing the resources given by cloud providers catering to its user's needs like scalability, usability, resource requirements. The US National Institute of Standards and Technology (NIST) defines it as follows [1]: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing allows users to access software applications and computing services. They might be stored off-site at locations rather than at local data centre or the user's computer [4]. Cloud computing caters to users' request for services. There is no need to spend money on purchasing and managing of resources. The three widely referenced cloud computing service models are explained as follows.

1. Software as a Service (SaaS): Also known as Application Service Provider or ASP model. It refers to service that gives users' the efficacy to access services of cloud by running simple software like a browse. Examples: Gmail, Google Groups.
2. Platform as a Service (Paas): This service allows the users' to develop applications and deploy them. Examples: Google App Engine allows developers to create customised apps.
3. Infrastructure as a Service (IaaS): This service allows users' to access the servers' computational and storage infrastructure in a centralized service [2] [3] [6]. Say for an example, we have Amazon Web Services. It allows remote access to Amazon.com's computing services.

In Cloud computing domain, there are set of important policies, which include issues of privacy, anonymity, security, liability and reliability [2]. The most important of these issues is the data security and how cloud providers assures it [2]. Most effective technique to protect our data is its encryption. Different encryption schemes for protection of data have been in use for many decades. Encryption of data is done by converting data from normal plaintext to unreadable cipher text. This tactic, however, doesn't prove to be much effective for cloud systems as this conversion involves huge and very complex mathematical computations.

II. Issues in Cloud Security

The three issues of cloud computing security are: confidentiality, integrity and availability; known as the ACI triad [3].

A. Availability

Availability is the attestation that data will be available to the user in a perpetual manner irrespective of location of the user. It is ensured by: fault tolerance, network security and authentication.

B. Integrity

Integrity is the assurance that the data sent is same as the message received and it is not altered in between. Integrity is infringed if the transmitted message is not same as received one. It is ensured by: Firewalls and intrusion detection.

C. Confidentiality

Confidentiality is avoidance of unauthorized exposé of user data. It is ensured by: security protocols, authentication services and data encryption services.

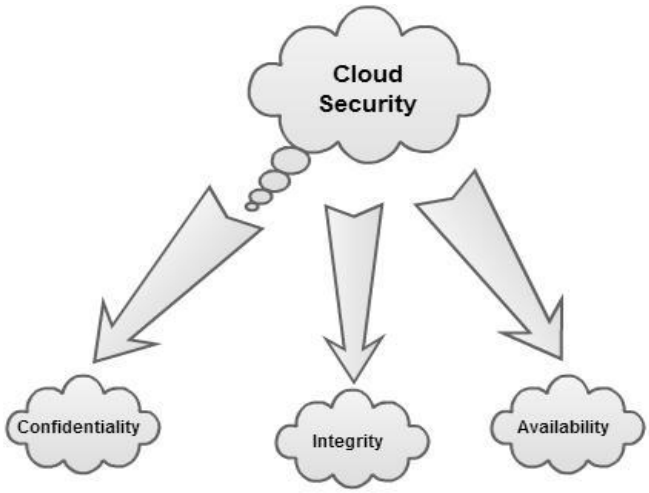

Fig 1: The AIC Triad

Since cloud computing is utility available on internet, so various issues like user privacy, data theft and leakage and unauthenticated accesses are raised [6]. Cryptography is the science of securely transmitting and retrieving information using an insecure channel [9]. It involves two processes: encryption and decryption. Encryption is a process in which sender converts data in form of an unintelligible string or cipher text for transmission, so that an eavesdropper could not know about the sent data. Decryption is just the reverse of encryption. The receiver transforms sender's cipher text into a meaningful text known as plaintext [13].

III. Literature Review

In 2010, Joshi et al. [1] provide an overview of different data security issues related to cloud computing. This piece of work focuses on ensuring security in cloud computing by providing secured trustworthy cloud environment. Farzad Sabahi [2] explains about the scope of various enterprises migrating to cloud. The author explains how migration to cloud can benefit various enterprises. Cloud computing migration involves considering the gravity of issue of security. In 2011, Ashish Agarwal et al. [3] talk about security issues concerned with cloud computing. This paper has talked about some serious security threats that prevails this field. Ashutosh Kumar et al. [4] focussed on providing a secure architectural framework for sharing and data gathering. This cynosure of this work is that the authors have made a permission hierarchy at different levels. The authors have focussed on security but with view of use hierarchy. In 2012, M.Venkatesh el al [5] proposes RSASS system for data security. The scheme uses RSA algorithm for encrypting large files and storing the date. The system can be used for storing large databases. But the use of linear methods compromises with the data retrieval speed. Hence, this system is good for static data. Prashant Rewagad et al. [6] propose a system for providing security in cloud network. The architecture uses the combination of digital signature algorithm of Diffie Hellman and AES encryption.

IV. Problem Statement

The security of data of the user is prime responsibility of cloud provider. So, for efficient data security we need a mechanism that provides secure data encryption as well as secure shield against data theft. The related works mentioned above have focussed on cloud security issues. They have provided different mechanisms for data security in cloud environment. Different researches have focussed on the fact that user generally has to access large volumes of data from the cloud in a secured manner. But the complexity of the cryptographic algorithm used, hasn't been given much importance. The complexity of the algorithm directly affects the speed of data access. We need some algorithm that will help in efficient and speedy secured data access.

V. Elliptic Curve Cryptography

1. Overview

Elliptic Curve Cryptography (ECC) was proposed by Koblitz [14] and Miller [15] in 1980s. ECC is a public key cryptographic scheme. It uses properties of Elliptic Curves to develop cryptographic algorithms. Security of ECC is based on the intractability of ECDLP i.e. Elliptic Curve Discrete Logarithm Problem. Elliptic Curve Cryptography is defined with help of following parameters as:

$$P = (q, FR, a, b, c, G, n, h) \quad (1)$$

q: the prime umber or 2m that defines curve's form. FR: field representation. a, b: the curve coefficients. G: the base point (Gx, Gy). n: the order of G. It must be big prime number. h: cofactor co-efficient [7] [12].

Elliptic Curves (EC) over finite fields are used to implement public-key protocols. The Elliptic curve is defined on either prime field GF (p) or binary field GF (2n). Since arithmetic in latter field is much faster, we work in GF (2n). An elliptic curve E is defined by the simplified projective coordinates as follow:

$$Y2Z + XYZ = X3 + aX2Z + bZ3 \quad (2)$$

This public key cryptography scheme is defined over two fields: prime Galois Field, GF (p), or over binary extension Galois Field, GF (2m). In GF (p), the equation of Elliptic Curve is:

$$Y2 \bmod p = x3 + ax + b \bmod p \quad (3)$$

Where:

$$4a3 + 27b2 \bmod p \neq 0 \quad (4)$$

with elements of GF (p) as integers between 0 and p-1 [7]. In GF (2m), the equation of Elliptic Curve is given by:

$$y2 + xy = x2 + ax2 + b \quad (5)$$

where: $b \neq 0$. Over GF (2m), rules for point addition and point doubling can be implemented [12] [14] [15].

2. Elliptic Curves on R

Elliptic curves, known and studied since centuries, used by Andrew Wiles in his proof of Fermat's last theorem are algebraic curves or Weierstra curves.

$$y^2 = x^3+ax+b$$

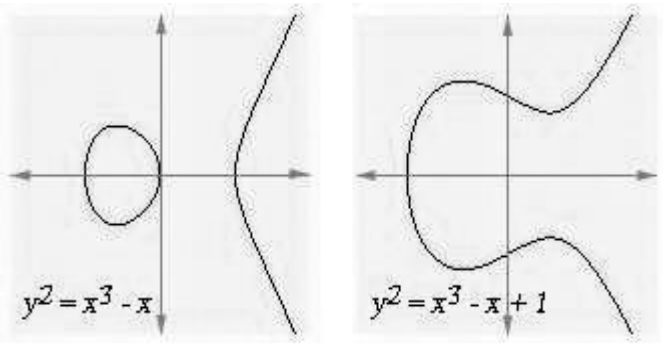

Fig 2: Elliptic curves for two equations

3. Discrete Logarithm Problem (DLP)

Elliptic curve system is based on DLP. A group structure given by elliptic curves over finite field is used to implement these schemes. Group elements are some rational points lying curve. They have a special point called point at infinity [7] [10] [11]. The group operation is addition of points. It is carried out by arithmetic operations in finite field. Major building block of ECC is scalar point multiplication. We take a point P and add it to itself. This operation is performed some n no of times to get resulted point Q. Number of times P is added is called k. To obtain k from Q and P is called as Elliptic Curve Discrete Logarithm Problem (ECDLP).

4. Advantages

Till date, there is no sub exponential-time algorithm to solve ECDLP in selected elliptic curve group .. Hence, cryptosystems that rely on ECDLP provide high strength-per-bit. This makes ECC work on smaller key sizes. It requires less memory than other DLP-based systems. The general key size for ECC is around 163 bits, providing the same security level as 1024 key bits of RSA. This makes ECC's very attractive for implementations in areas where we have memory limitations and computational overhead is a concern.

VI. Diffie Hellmann Key Exchange

Diffie-Hellman key exchange protocol is first public key cryptography scheme. It was proposed by Witfield Diffie and Martin Hellman in 1976 [8]. It uses two keys -- one secret and other private key. If Sender wants to communicate with the receiver, he encrypts the message with his private key and senders' public key. On the receiving end, receiver decrypts the sent message using his private key and sender's public key [8] [13]. This scheme is based on the difficulty of computing logarithmic functions for prime exponents. This is known as Discrete Logarithm Problem (DLP) [11].

VII. Proposed System

In this paper we aim at removing the security threats for cloud architecture by using two encrypting techniques: Diffie Hellmann Key Exchange and Elliptic Curve Cryptography. To deploy these two methods, we have proposed a new architecture which can be used to design a cloud system for better security and reliability on the cloud servers at the same time maintaining the data integrity from user point of view.
Our system involves following steps:

1. Establishment of connection

As soon as the user logs in our system for the first time, he is asked to make an account in the system. The initial connection is established with the help of HTTPS and SSL protocols.

2. Account Creation

For the first time when a secured connection is formed, the user is asked to fill in the account details required for account creation in our cloud system. These details are sent over the internet to our server. The account is created in the system. Further, the connection is then established by Diffie Hellmann Key Exchange protocol. The server also generates the user id which acts as unique user identifier, its Diffie Hellman equivalent stream, required private and public key for ECC encryption. The user id is sent to the user over the secured channel.
User is asked to keep this id as a secret because it is used as a tool to authenticate him every time he logs on to the system.

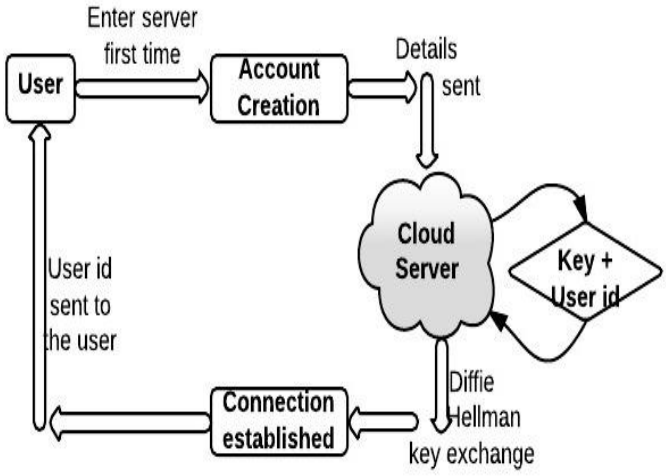

Fig 3: Account creation process

3. Authentication

As soon as the user opens the home page of cloud server, SSL connection is established. As the account is created, the user is asked to authenticate himself giving all the necessary details and the secret user id sent to him earlier.
The cloud server checks the validity of user by first finding out the Diffie Hellman equivalent of the user id from the server repository. If the key matches, then the connection is established by this protocol again and user is logged in to the

server. At the back end of user, its private key and the ECC algorithm is sent for encryption.

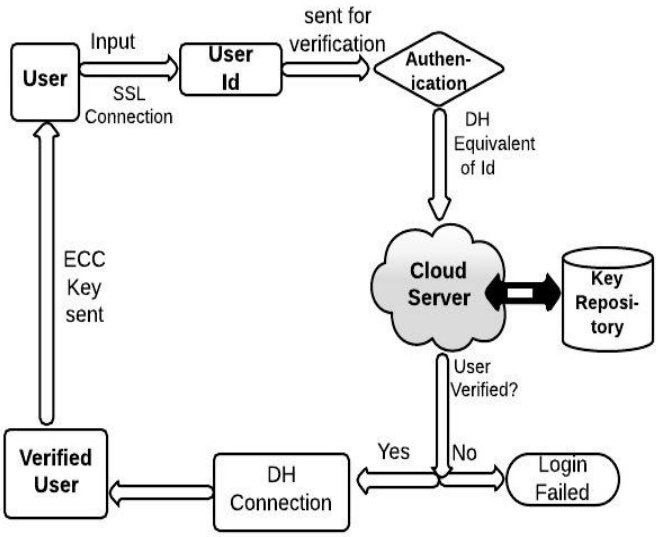

Fig 4: Authentication of user

4. Data Exchange

The data exchange here includes 2 steps:

A. The client side: The client wants to fetch a data from server repository; his query is converted in a form of file and encrypted using his public key. This encrypted data is then sent to client for processing.

B. The server side: The server receives the encrypted data. It decrypts it using the private key and processes user query. The result of so obtained is encrypted again and sent to the client side.

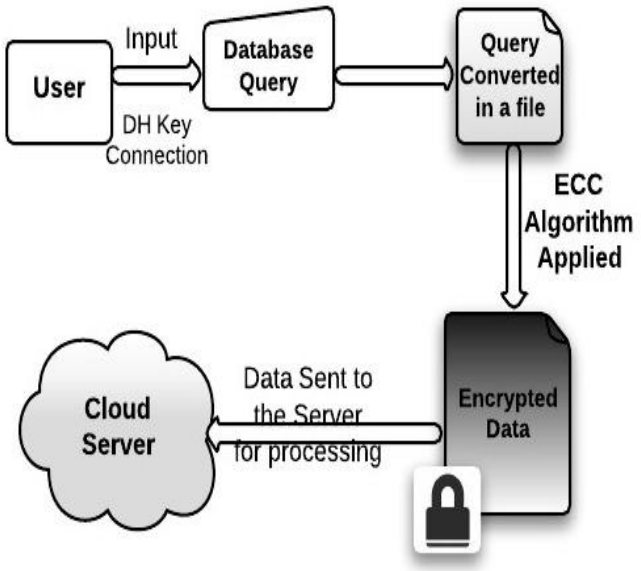

Fig 5: Data Processing view of Client

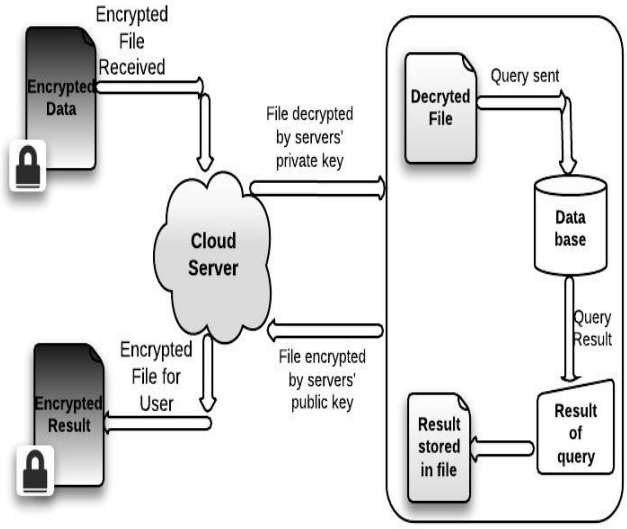

Fig 6: Data Processing view of Server

VIII. COMPUTATION OF KEY FOR CRYPTOGRAPHY

The key generation in this architecture takes place at two levels: one for ECC and other for Diffie Hellman.

1. For ECC

The public key is point on the curve. Private key is a random number. The public key is generated by multiplying private key with generator point G [11]. This point generation and other factors are discussed below.

A. Computation of Point on the Curve

ECC algorithm has the ability to compute a new point on the curve given the product points. We encrypt this point as information to be exchanged between the end users [9].

B. Choice of Field

To analyse algorithms with smaller computations, we use polynomial time algorithms and for complex computations can be evaluated with exponential time algorithms [9]. The equation of an elliptic curve is given as,

$$y2 = x3 + ax + b$$

C. Integer Factorization

Given an integer n which is the product of two large primes' p and q, we have:

$$y2 = x3 + ax + b$$

It is easy to calculate n for given p and q. It is computationally infeasible to determine p and q for large values of n. Its security depends on the difficulty of factoring the large prime numbers. The method used to solve Integer Factorization problem is the Number Field Sieve which is sub exponential algorithm [11].

D. Key Generation

Key generation is an important part. An algorithm should generate both public and private key. The sender will encrypt the message data with the receiver's public key and receiver will decrypt with its private key. Select a number, d in range of n. We generate the public key using following equation,

$$Q = d * P$$

d = the random number in range of (1 to n-1). P is a point on curve. Q is public key. d is private key.

E. Encryption

Let 'm' be message to be sent. Consider 'm' has point 'M' on the curve 'E'. Randomly select a value 'k' from [1 - (n-1)]. Two cipher texts will be generated let it be B1 and B2.

$$B1 = k * P$$
$$B2 = M + (k * P)$$

F. Decryption

Use the following equation to obtain original message that was sent i.e 'm'.

$$M = B2 - d * B$$

M is original data that was sent.

2. Diffie Hellman Key Exchange

This protocol is one of the pioneers in birth of public key cryptography. It follows the following steps.

Input: G is an abelian group;

g $\in$ G, m is prime multiplicative order.

Output: A secret s $\in$ G which will be shared by both the sides.

Steps:

Sender generates random d_A $\in$ {2,....,m-1} and compute $e_A = g^d_A$.

Sender sends e_A to receiver.

Receiver generates a random d^B $\in$ {2,....,m-1} and computes $e_B = g^d_B$.

Receiver sends e_B to receiver.

Sender calculates $s = (e_B)^d_A = g^{d_A d_B}$

Receiver calculates $s = (e_A)^d_B = g^{d_A d_B}$

IX. Conclusion and Future Scope

In this paper, we have analysed the security issues faced by user's private data in the cloud system and the inevitable need to find a solution to the problem. Data security can be very well assured by use of linear cryptographic algorithms but the massive amount of data in cloud computing put a hindrance to the idea. So, we have proposed an architecture which can be implemented in cloud environment taking the advantages of linear cryptography for establishing a secure connection and exponential cryptography for encrypting the data. The two algorithms used are Diffie Hellman Key Exchange and Elliptical Curve Cryptography. With help of these two algorithms, we provide a four step procedure for ensuring authenticity of user. The first step is to establish the connection, second is account creation, third is authentication and last one is data exchange. We have used ECC because its computational cost as well as speed of this algorithm is very less compared to linear algorithms present. One more advantage is that it has a sub exponential time complexity which makes it difficult to crack. We have used Diffie Hellman protocol as it significantly better for establishment of connections.

In future, we emphasize on the implementation of the proposed architecture along with different comparisons to show the effectiveness of our proposed architecture.

X. References

[1] Joshi, J.B.D., Gail-Joon Ahn. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security Privacy Magazine, Vol 8, IEEE Computer Society, 2010, p.24-31.

[2] Farzad Sabahi. Cloud Computing Security Threats and Responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference.

[3] Ashish Agarwal, Aparna Agarwal. The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences [VOL I, SPECIAL ISSUE ON CNS, JULY 2011] [ISSN: 2231-4946].

[4] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava. Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment. Software Engineering (CONSEG), CSI Sixth International Conference, Sept. 2012

[5] M.Venkatesh, M.R.Sumalatha, Mr.C.SelvaKumar. Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing. Recent Trends In Information Technology (ICRTIT), 2012 International Conference, April 2012.

[6] Prashant Rewagad, Yogita Pawar in. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.

[7] Hai Yan, Zhijie Jerry Shi. Software Implementations of Elliptic Curve Cryptography. Information Technology: New Generations, Third International Conference, April 2006.

[8] W. Diffie and M.E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 1976.

[9] Ravi Gharshi, Suresha. Enhancing Security in Cloud Storage using ECC Algorithm. International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 7, July 2013.

[10] H. Modares, M. T. Shahgoli, H. Keshavarz, A. Moravejosharieh, R. Salleh. Make a Secure Connection Using Elliptic Curve Digital Signature. International Journal of Scientific & Engineering Research Volume 3, Issue 9, September-2012 ISSN 2229-5518 IJSER © 2012.

[11] Aqeel Khalique Kuldip Singh Sandeep Sood. Implementation of Elliptic Curve Digital Signature Algorithm. International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010

[12] Alfred Menezes, Minghua Qu, Doug Stinson, Yongge Wang. Evaluation of Security Level of Cryptography: ECDSA Signature Scheme. Certicom Research. January 15, 2001.

[13] W. Stallings. Cryptography and Network Security: Principles and Practice. (3rd ed.). Prentice Hall, Upper Saddle River, New Jersey, 2003.

[14] Koblitz, N., 1987. Elliptic curve cryptosystems. Mathematics of Computation 48, 203-209.

[15] Miller, V., 1985. Use of elliptic curves in cryptography. CRYPTO 85.